

SUBSTITUTE SPECIFICATION

[ATTACHMENT 1 TO THE FIRST PRELIMINARY AMENDMENT FILED IN CONTINUATION
APPLICATION TO U.S. PATENT APPLICATION 09/523,387.]

09/523,387

**A METHOD AND APPARATUS FOR DYNAMICALLY DRILLING-DOWN
THROUGH A HEALTH MONITORING MAP TO DETERMINE THE HEALTH
STATUS AND CAUSE OF HEALTH PROBLEMS ASSOCIATED WITH
NETWORK OBJECTS OF A MANAGED NETWORK ENVIRONMENT**

5

RELATED APPLICATIONS

[0001] The present invention is a continuation of copending U.S. Patent Application No. 09/523,387 filed on March 10, 2000, which is a continuation-in-part of U.S. Patent Application 09/087,338 filed on May 29, 1998.

10

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention relates generally to network management, and more particularly, to monitoring health problems of network devices and services of a managed network environment.

Related Art

[0003] As computer networks have become more prevalent in corporate and other operating environments, network management software that is capable of solving network problems automatically and remotely has become more crucial. One of the major goals of any efficient network administration setup is the specification and measurement of acceptable performance thresholds for each machine in the network without creating additional network traffic. Network management software typically manages and automates administrative tasks across multiple machines in a network. Typical network management software allows administrators to measure log events and view status when performance criteria is not acceptable. Unfortunately, however, the administrator is often not informed of problems on the network by network management software until after one or more end users of the network has been affected

[0004] Accordingly, there exists a need in the art for a proactive diagnosis of network management problems in a timely manner. There is further a need for a complete, global view of the network environment, including a view of all critical components. There exists a need to quickly display to the administrator of a network health problems associated with devices and services on the network and provide the capability of the administrator to quickly respond to and correct pending network problems before end users of the network are impacted.

[0005] The Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP) are network management protocols that provide a generic mechanism by which different manufacturers' equipment and/or services can be monitored and controlled from a management system, such as a UNIX server. A network component or service provided on a managed network can be monitored and controlled using a management protocol to communicate management information between network components and services on the network. A network component can include networked personal computers, workstations, servers, routers, bridges, print servers, print queues, and printers. Network services, particularly in an Internet environment, can include electronic mail (e-mail), browsers, and service level agreements. There exist several key areas of network management including fault management, configuration management, security management, performance management, and accounting management. With the ability to instruct a network component to report events and the ability to start processes on a network component, the network can be manipulated to suit changing conditions within a network system.

[0006] A key mechanism by which various network devices communicate with a management system is via SNMP traps or CMIP events. Hereafter, "events" will be used to refer to either SNMP traps or CMIP events. Events allow for unsolicited notifications to be sent from one network device or service to another. This same mechanism can be used for communication between various cooperating software components within the management system.

[0007] There are several software products that receive events and allow a user to manage network devices. One of these products, Network Node Manager (NNM) from Hewlett-Packard Company of Palo Alto, CA., enables a user to manage network devices

using a graphical user interface (GUI) along with graphically representing relationships between network devices. Hereafter "NNM" will be used to generically refer to a product that receives events and allows a user to manage network devices, such as HP's Network Node Manager. From the NNM console, a user is able to discover and display all of the network devices on the network and to proactively monitor and manage all servers on the network. This makes it easy to determine the network status or to follow the path of a failed print job, for instance, and determine the point at which it failed. Because it is easy for a user to see how a network is configured, it is easy to manage network devices and optimize the configuration. For instance, a configuration may be optimized by balancing the number of print queues per print server or the number of print servers per file server. Any network device may be managed by an NNM such as NetWare® file servers, print servers, print queues, and printers. (NetWare is a trademark of Novell, Inc.) During initialization of the NNM, network devices are automatically discovered and added to a topology database. Each network device is graphically represented by an icon on the NNM console. Using NNM, a user can proactively monitor and manage all network devices on a managed network. A user can monitor the state on a network device over various periods of time by keeping trend data. A user can use trend thresholds to troubleshoot problems on network devices or to plan future expansion of network devices, such as increasing volume and disk sizes, or increasing the number of users allowed access to a server at one time.

[0008] All events are assigned a default severity which can be overridden by the user. The NNM utilizes registration files for user configurable information. The severity level of each event that is received by the NNM that corresponds to a particular network device is represented by a unique color. The severity level of a network device is indicated on the NNM console by the color of the network device's icon. A critical event, for instance, is depicted with a red icon. For instance, by default, a critical event is indicated to the user when a network device icon on the NNM map changes color to red indicating a critical status related to that network device. Thus, the current status of the entire network can be easily inspected by a user using the color status indications of the network device icons.

[0009] While the occurrence of a critical event for a network device is depicted by a red icon or other indication for that device, the simple color indication of a red icon, for instance, does not, in and of itself, communicate to the user exactly the nature of the critical event that caused the icon to change to a red color. There is an unmet need in the art for a user, such as an administrator of the network environment, to be able to not only know that the icon for a particular device indicates the occurrence of a critical event, but to also be able to quickly and readily ascertain the exact nature of that critical event.

[0010] Network printers are graphically represented with a printer icon representing each of the network printers on the network. A user can remotely determine the "health" status of any of the network printers visually. The LED status on the network printer can then be browsed to determine if the printer needs to be serviced or if human intervention is required. For instance, it can be determined if a printer has any of the following problems: Out of paper; Out of ink; Paper jam; Door open; Toner low; Printer problem; and Bin full. A drawback of this approach, however, is that the exact nature of the critical event, e.g. door open, has to be determined by looking at the problem network printer device itself and cannot be determined remotely by looking at the red color icon of the problem network printer on the NNM network console.

[0011] Servers are graphically represented with a server icon representing each of the servers on the network. A server running the appropriate agent software may be managed by a user from the NNM console. A server running the appropriate agent software responds to management data requests from the NNM console and transmits alarms from the server to the NNM console. This makes it possible for the NNM to display real-time server performance and configuration data on those servers and to monitor key performance statistics including: CPU utilization; number of users; number of connections; memory usage and configuration; installed software; and disk and volume usage. Thresholds can be set on these parameters to cause an SNMP trap, or they can be graphed by the NNM to evaluate history or trends. Parts of a server may also be viewed when troubleshooting a problem. Viewing components of a server's configuration (the network interfaces, for example) might help solve a critical problem with the server.

[0012] Server faults may be managed by monitoring key parameters of the servers, such as CPU load and available disk space, as well as noting significant events, such as

NetWare Loadable Modules (NLMs) being unloaded or trustee rights changing. These conditions may be monitored directly at the servers and passed to the NNM via SNMP traps. For file servers, a user can obtain current and historical trend data and set alarm thresholds for trend parameters so that the user is notified when a threshold is passed.

- 5 [0013] Novell's NetWare Management Agent (NMA) Management Information Base (MIBs) and trap definitions are integrated into NNM. NNM may be configured to integrate the NMA traps with associated Novel "NetExpert" help text. When an SNMP alarm is sent to an NNM console, the alarm can be reviewed for more detailed help text describing the problem. The alarm, however, is not directly correlated to the red icon
- 10 indicating that a particular network device is having a problem. This means that the process of reviewing the alarm sent to the NNM console is separate from the process of viewing a red icon on the NNM console and that these processes are not correlated. The user can also followed detailed instructions that guide the user through a series of steps to resolve the problem discovered by the NMA agent.
- 15 [0014] Referring to Figure 3, IP-centric group views 60 for graphically displaying network devices, according to the prior art, is shown. User interface 62 contains a representation of the network indicated by IP Internet icon 64. Double-clicking the IP Internet icon 64 will result in the presentation of user interface 66 having containers 68, 70 for the group views of the network indicated by NW-Servers:GOTO icon 68 and
- 20 NT-Servers:GOTO icon 70. Double-clicking on NW-Servers:GOTO icon 68 will result in the presentation of user interface 72 containing the NW-Server-related network devices discovered by NNM during initialization. Three NW-Server-related network device icons are shown each representing individual network devices: nwstrn0a icon 74, nwstrn0b icon 76, and nsmdem3 icon 78. This group view configuration is considered IP-centric
- 25 (Internet Protocol Centric) because during network device discovery all network devices are initially contained in a single group view that is presented by double-clicking on the IP Internet icon 64. A user may manually construct basic group views such as NW-Servers and NT-Servers as shown as NW-Servers:GOTO icon 68 and NT-Servers:GOTO icon 70, respectively.
- 30 [0015] NodeView is a product that enhances products that receive events and allow a user to manage network devices such as NNM. Using NodeView, related network

devices are automatically grouped into maps represented by group icons. Group views are hardwired into the NodeView code itself. Referring to Figure 4, device-centric group views 80 for graphically displaying network devices, according to the prior art, is shown. User interface 82 contains a representation of the network on top of background 91, a map of the United States. The top-level network is indicated by Internet icon 84. The group views of the network are represented by NW-Servers icon 90, NT-Servers icon 92, Web-Servers icon 86, HP-Printers icon 88, and DMI-Clients icon 94. This group view configuration is considered device-centric because during network device discovery related network devices are automatically grouped into group views represented by group view icons. Double clicking on a group icon will explode a map, hereafter referred to as a "group view", showing all the related devices that were previously discovered in the topology database. For instance, double-clicking on NW-Servers icon 90 will explode to a NetWare Servers group view showing all of the NetWare servers that were discovered in the topology database. A group view of related devices provides a user with a simple way to monitor and launch applications using the menubar and NetWare tool launcher from a single view of the managed environment. The menubars, popup menus, and toolbar remain consistent for each of the group views provided by NodeView.

[0016] In the prior art, the group views are hardwired into the NodeView code itself. This means that a NodeView user cannot select his/her own choices for group views nor dynamically update this selection. There is therefore an unmet need in the art to allow a user to be able to dynamically configure group view information. Additionally, the menubars, popup menus, and toolbar are not individually configured for a selected group view, but rather remain consistent regardless of whether an item is only applicable for certain group views and meaningless for others. There is therefore an unmet need in the art to allow the menubars, popup menus, and toolbar to be context sensitive to the group view.

SUMMARY OF THE INVENTION

[0017] It is therefore an object of the present invention to quickly display to the administrator of a managed network health problems associated with devices and services

on the network and to provide the administrator with the capability to quickly respond to and correct pending network problems before end users of the network are impacted.

[0018] It is a further object of the present invention to allow for a proactive diagnosis of network management problems in a timely manner.

5 [0019] It is another object of the present to provide a complete, global view of the network environment, including the ability to provide a view of all critical components readily upon demand, to allow for this proactive diagnosis.

[0020] It is yet another object of the present invention to be able to readily and quickly ascertain the exact nature of a critical event that caused an icon representative of a
10 network device or service to change to indicate the occurrence of the critical event.

[0021] Therefore, according to the present invention, user-configurable group views allow an administrator of the network, upon noticing that an icon is indicative of a critical event having occurred, as reflected in the color, shape, or other such indicator of the icon, to "drill down" via a user interface to the network device or service that is the
15 subject of the critical event and to then view an event or trap message associated with the critical event that is stored as a field of the network device or service effected by the critical event. According to the methodology of the present invention, health characteristics of each network object of interest in the network environment that determine the health status of each network object are defined. Each network object is
20 grouped in a group view with other network objects that share attribute values that define the group view. The health characteristics of each network object are monitored in order to determine the health status of each health characteristic of each network object. Moreover, the health characteristics are stored in a health characteristic configuration file, such as a registration file, of a group view with which the network object it is associated
25 with belongs. Group view containers of a map, each corresponding to a group view having a number of network objects within it all sharing common group attribute values, are displayed within the user interface. The health characteristics, the network objects, and the group view containers each have health status indicators that reflect health status. Health status indicators are intended to quickly convey to the user of the managed
30 network, such as the administrator of the network, when a group view container, network object, or health characteristic is in poor health and may include the color or shape of an

icon or an audible alarm. Determining the health status of each health characteristic includes comparing performance data of the health characteristic to a predetermined threshold of the health characteristic, and then, if the performance data of the health characteristic violates the predetermined threshold of the health characteristic, causing the health status indicator of the health characteristic to indicate a poor health condition of the health characteristic. Each group view displayed within the map that has a poor health status is identified by the health status indicator of its container. Selecting the container having a poor health indication, will cause the group view of that container to be displayed within the user interface. The user can quickly tell which of the network objects of the group view have poor health from the health status indicators of the network objects. Selecting the one or more objects having poor health will cause the health characteristics of the problem network objects to be displayed in the user interface. The one or more health characteristics having health problems, as indicated by the health status indicators of the health characteristics, can then be selected to cause a message to be displayed in the user interface that identified the event that caused the poor health status of each health characteristic of concern.

[0022] The drill-down of the present invention to determine the underlying, root cause of a poor health status need not start at the group view container level of the network hierarchy. If the user of the system is already viewing the network objects of a particular group view or the health characteristics of a particular network object, for instance, the drill-down would commence at that level.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The novel features believed characteristic of the invention are set forth in the claims. The invention itself, however, as well as the preferred mode of use, and further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawing(s), wherein:

[0024] Figure 1a illustrates a flow chart of dynamically adding group views, according to the present invention;

[0025] Figure 1b illustrates a flow chart of dynamically modifying group views, according to the present invention;

[0026] Figure 1c illustrates a flow chart of dynamically deleting group views, according to the present invention;

5 [0027] Figure 2 illustrates a flow chart of the context sensitive menubars, popup menus, and toolbar, according to the present invention;

[0028] Figure 3 illustrates IP-centric group views for graphically displaying network devices, according to the prior art; Figure 4 illustrates device-centric group views for graphically displaying related network devices, according to the prior art;

10 [0029] Figure 5 illustrates a menubar that is context sensitive to the group view that is selected, according to the present invention;

[0030] Figure 6 illustrates editing group view information that is stored in a file using a graphically interface, according to the present invention

15 [0031] Figure 7 illustrates of flow chart of dynamically drilling-down through a hierarchy of maps and sub-maps of a managed network to determine health status and causes of health problems associated with network objects of the managed network, according to the present invention;

[0032] Figure 8 illustrates a flow chart of determining health status of health characteristics of network objects, according to the present invention;

20 [0033] Figure 9 illustrates a group view container and group view Internet map within a graphical user interface, in accordance with an embodiment of the present invention;

[0034] Figure 10 illustrates a group view sub-map containing health status information, in accordance with the present invention;

25 [0035] Figure 11 illustrates the health characteristics of a network object, in accordance with the present invention; Figure 12 illustrates a user interface that contains a message communicating the cause of a health problem of a network object, in accordance with the present invention; and

[0036] Figure 13 illustrates contents of a registration file of user-configurable group views, in accordance with the present invention.

DESCRIPTION OF THE INVENTION

5 [0037] The present invention stores group view information, called group view attributes, in a file that may be edited by a NNM user so that a user can dynamically configure group view information. Group view attributes that may be edited include: the name of the group view, the background graphic image, the symbol type, and the context
10 of the group view. NodeView utilizes registration files to create context sensitive group views such that only those items of a menubar, popup menu, or toolbar that are registered to a particular group view are shown when that group view is selected by the user. These user-configurable group views allow an administrator of the network, upon noticing that an icon is indicative of a critical event having occurred, as reflected in the color, shape, or
15 other such indicator of the icon, to "drill down" to the network device or service that is the subject of the critical event and to then view an event or trap message associated with the critical event that is stored as a field of the network device or service effected by the critical event.

[0038] Referring to Figure 1a, a flow chart of dynamically adding group views 10,
20 according to one embodiment of the present invention, is shown. Initially, the user is presented with a list of group views at Block 12. The user selects to add a group view at Block 14. The user enters new group view information at Block 16. At Block 18 the new group view is added to the list of group views. Finally, at Block 20, the user is presented with a list of group views including the new group view.

25 [0039] Referring to Figure 1b, a flow chart of dynamically modifying group views 30, according to the present invention, is shown. Initially, the user is presented with a list of group views at Block 32. The user selects to modify a group view at Block 34. The user modifies the group view information at Block 36. The user is again presented with a list of group views at Block 38.

[0040] Referring to Figure 1c, a flow chart of dynamically deleting group views 40, according to the present invention, is shown. Initially, the user is presented with a list of group views at Block 42. The user selects to delete a group view at Block 44. The user is presented with a list of the remaining group views at Block 46.

5 [0041] Referring to Figure 2, a flow chart of the context sensitive menubars, popup menus, and toolbar 50, according to the present invention, is shown. The user opens a group view, at Block 52, by double-clicking on the group view icon. A lookup is performed on a NodeView registration file for the context sensitive information for that group view at Block 54. The menubars, popup menus, and toolbar for that group view are
10 modified at Block 56.

[0042] Referring to Figure 5, a menubar that is context sensitive to the group view that is selected according to the present invention, is shown. Double-clicking on NW-Servers icon 90 will result in the presentation of user interface 102 containing the NW-Servers-related network devices discovered by the NodeView-enhanced NNM during
15 initialization. Selecting menubar 104 will result in the presentation of a menubar that is context sensitive to the group view selected, in this case NW-Servers.

[0043] Referring to Figure 6, an illustration of editing group view information, stored in a file, using a graphical user interface 110, according to the present invention, is shown. Selecting map properties from the menubar will result in the presentation of user
20 interface 112 containing Configurable Applications selection list 114. Selecting NodeView from the Configurable Applications selection list 114 will result in the presentation of user interface 116 containing the group view attribute list 118. Group attributes are listed by name 120 and value 122. A group view attribute may be edited by selecting a group view attribute from the group view attribute list 118 and modifying that
25 group view attribute's value.

[0044] The user-configurable group views described above allow an administrator of the network, upon noticing that an icon of a user interface of the NNM console is indicative of a critical event having occurred, as reflected in the color, shape, or other such indicator of the icon, to "drill down" to the network device or service (object) that is
30 the subject of the critical event and to then view an event or trap message associated with

the critical event that is stored as a field of the network device or service effected by the critical event.

[0045] Referring now to Figure 7, the general methodology 130 of a preferred embodiment of the present invention for proactively determining health status of network objects and user-configurable group views of a windows-based managed network environment is shown. It is noted at the outset of the description of Figure 7, that not all steps shown therein are necessarily performed in order to determine the root cause of concern; the amount of drill-down that is required is a function of where in the hierarchy of maps and sub-maps the administrator is located when initially alerted to the presence of a network object in poor health. Similarly, additional steps that those detailed in Figure 7 may be required if the hierarchy of maps and sub-maps of the managed network so dictates; this is accomplished without departing from the spirit and scope of the invention. At Block 140, one or more health characteristics are defined for each network object of interest in the managed network environment.

[0046] As previously stated, network objects of the managed network environment may include network devices such as personal computers, workstations, servers, routers, printers, bridges, etc. and network services such as the Internet and electronic mail. Health characteristics, referred to as "Health Indicators" in the figures, provide information about the health of a particular network object and can include CPU utilization, memory utilization, network utilization, and disk utilization. For instance, if the network object is a network server, for instance, health characteristics may include disk utilization, memory utilization, network utilization, and processor utilization. The health status of each health characteristic of the network object of interest must be determined at Block 150. Each health characteristic has a health status that is reflected in a health status indicator; the health status of each health characteristic of a network object is used to determine the health status of the network object, and the health status of each network object of a grouped view (sub-map) is in turn used to determine the overall health status of that group view

[0047] In the preferred embodiment of the present invention, determining the health status of each health characteristic is accomplished in the manner set forth in the methodology 150 of Figure 8 by monitoring the health indicators previously defined. At

Block 152, performance data related to the health characteristic of the network object of interest is compared to a preset (predetermined) threshold value of that health characteristic to determine if there is a problem. As an example, when a service level availability threshold in an electronic mail, Internet environment is violated (such that there is less than 90% availability for e-mail), health status indicators notify the administrator of the existence of a problem so that its root cause may be determined timely by drilling down through any sub-maps that exist in the hierarchy of the network.

[0048] If the performance data indicates that performance of the network object, as indicated by the performance data violating the preset threshold value for that health characteristic at Block 154, then the health status indicator of that health characteristic is changed to reflect a poor health status at Block 158. If, however, the performance data does not violate the threshold value then the health status indicator of the health characteristic is reflective of a good health status at Block 156. The health status indicator of a health characteristic may be a color of an icon of the health characteristic, a shape of the icon of the health characteristic, a sound associated with the health characteristic, or other appropriate indicators of health. For instance, the health status indicator may be the color red for the health characteristic icon of interest, the health characteristic icon shaped like a stop sign, or an audible alarm.

[0049] Moreover, indicators capable of communicating varying degrees of trouble may be utilized. Thus, a red icon may be used to indicate a more serious health problem than an orange or yellow icon, for example. Referring back to Figure 7, at Block 160, the health indicators for each network object of interest are stored in a registration file of the appropriate group view; each group view has a registration file database used to store the attributes and health characteristics, or indicators, associated with all network objects within that group view. It is noted that the order of Blocks 150 and 160 of Figure 7 may be reversed without departing from the spirit and scope of the invention.

[0050] Once the health characteristics of the network objects of interest have been defined and their health status determined, then the "drill down" process of proactively determining problem network objects of the managed network environment may commence. The first step is for a user of the system, such as the system administrator, to have notification that there is a problem of some sort with the network so that the process

of proactively determining what the problem can begin. The initial indication of a network problem typically occurs at a high level and the system administrator would then "drill down" to find the specific cause of the problem using the user-configurable group views described earlier.

5 [0051] At Block 170, group view containers are displayed within a map of the user interface. Each group view container corresponds to a group view, or sub-map, in which network objects sharing the user-definable group view attributes described above and stored in a database are grouped. Each group view container displayed in the user interface has a group view health status indicator that is representative of the overall health status of its group view; the overall health status of the group view is determined by the health status of each network object of the network objects within the group view and the health status of each network object is determined by the health status of the health characteristics of a network object. As with the health status indicator of a health characteristic, the group view health status indicator may be color, shape, sound, or other indicator chosen to be appropriate to the particular network.

10 [0052] The user can select, through manipulation of the network user interface, one or more group view containers indicated to have an overall health problem at Block 180. Selection of the group view containers occurs within the preferred embodiment by clicking on the container of interest with a mouse within a window of a graphical user interface (GUI); one skilled in the art, however, will recognize that selection may occur through other means as well. Selection of a group view container causes the group view corresponding to that container to be displayed in the user interface. This is the first part of the drill-down process.

15 [0053] Because the group view container selected has an overall health problem as reflected in its group view health status indicator, at least one network object of the network objects displayed in the group view will also have poor health as reflected in the network object health status indicator of the network object. As with the health status indicator of a health characteristic and the group view health status indicator of a group view, a network object health status indicator may be color, shape, sound, or other indicator chosen to be appropriate to the particular network. At Block 190, the administrator or other user of the network will select the one or more network objects of

the group view having a health problem; this is the next step of the drill-down process. Selecting a problem network object will cause one or more health characteristics of the object to be displayed within the user interface; because the network object thus selected has a health problem, at least one of the health characteristics of the network object will in turn have a health status indicator indicative of poor health. The health of each health characteristic thus displayed may be quickly and easily ascertained by its health status indicator, whether that be color, shape, sound, etc.

[0054] Now that one or more health characteristics of a network object have been found to have poor health on the network, the next and final step is to ascertain the root cause of health problem. This is accomplished, at Block 200, by selecting the health characteristic of concern in order to determine its health problem. Selection of a problem health characteristic will cause a message, indicative of the root health problem, to be displayed within the user interface. Typically, the message will be a trap or event message reflective of the critical event that caused the health problem and is stored as a field of the network object.

[0055] The message may be generated for any event type, including SNMP traps and CMIP events. If the invention is being used as part of an alarm browser, such as in Internet applications, the trap message may be stored in the alarm browser.

[0056] It is noted that the administrator of the managed network is provided initial indication of a network problem via the health status indicators of either the group view containers, the network objects within the group view containers, or the health characteristics of the network objects. If the administrator is away from the NNM console, however, the occurrence of the performance data of a health characteristic of a network object violating a preset threshold value may operate to cause the administrator to be alerted at a remote location, such as by paging the administrator upon the occurrence of the critical event. This allows the critical event to be addressed as soon as possible in order to minimize negative impact on the end users of the network.

[0057] It is further noted that depending upon where the administrator is located within the hierarchy of maps (group view containers), sub-maps (group view of network objects), and health characteristics when performance of a network object fails to meet the preset standard for it, a complete drill-down may not be necessary to determine the root

cause of the failure. Thus, for instance, an administrator who is looking at a group view sub-map of print servers when a particular print server in that group view has an icon that changes from a green to a red state (change of its network object health status indicator) will be automatically alerted at that level of the hierarchy that a problem exists and thus a complete drill-down from the group view containers is not necessary. The administrator would simply select the problem print server to see which of its health characteristics is indicated as being in poor health. The problem with the health characteristic would be displayed in a trap message after selecting the problem health characteristic as described above. In this example, at least one step of drill-down is eliminated.

[0058] Similarly, if the administrator is already viewing the health characteristics of a particular network object when the health status indicator of one of the health characteristics indicates trouble, the user would only have to select the problem health characteristic to then immediately view a message in the user interface about the critical event. By the same token, the drill-down described in Figures 7 and 8 does not prevent the user of a larger hierarchy of maps and sub-maps to be employed. In fact, there may be additional hierarchical layers of maps and sub-maps beyond that reflected in flow 130 without departing from the spirit and scope of the invention.

[0059] An example of a specific implementation that might be used with the present invention is shown in Figures 9-13. In this example, the health status indicators for group view containers, group view network objects, and health characteristics are color-based. Referring now to Figure 9, a group view container and group view Internet map 210 within a graphical user interface 220 is shown. Map 210 illustrates a number of network objects, including Internet network devices 230, 232, 234, 236, 238, 240, 242, 244, and 246, as well as group view containers 248 and 250. All of the network objects in map 210 have a green health status indicator, except for 232 which is yellow; group view container 248 for ManageX-Servers has a brown indicator while group view container for MS Exchange-Servers 250 has a red indicator. Also illustrated are the alarm categories 215 utilized in an alarm browser on the Internet. Error Alarms, Status Alarms, and Application Alert are indicated by the color brown in the alarm browser. Threshold alarms and All alarms are indicated by the color red in the alarm browser. ManageX and MS Exchange alarms are indicated by green in the alarm browser.

[0060] Of particular concern in map 210 is ManageX-Servers group view container 250, which is red in color, an indication that there is a potentially serious health problem with one or more of the network objects contained within container 250.

Selecting container 250, such as by clicking on it, brings up the group view or sub-map 260 of the ManageX-Servers within the GUI 265 of Figure 10; this is the first drill-down step in this example. Within group view 260 there are shown three ManageX-Servers: hpdaver server 270, nnmrules server 290, and theforce server 280. At a glance, a network administrator can see which of the servers contained within group view 260 has a health problem. hpdaver and theforce servers 270, 280 are both green, while nnmrules server 290 is blue. The blue network object health status indicator of nnmrules server 290 is the color blue, an indication of a poor health condition in this example.

[0061] The administrator thus selects nnmrules server 290, such as by clicking on it with a point-and-click device, to drill-down to the health characteristics of this network device in Figure 11. Displayed within GUI 300 are various health characteristics 310:

nnmrules:CPU health characteristic 312, nnmrules:Disk health characteristic 314, nnmrules:Memory health characteristic 316, and nnmrules:Network health characteristic 318; as previously discussed, these health characteristics refer to CPU utilization, disk utilization, memory utilization, and network utilization, respectively. Only

nnmrules:CPU health characteristic 312 has a health status indicator that is red; the health status indicators of the other health characteristics are green. Since red denotes an alarm in this example, the administrator can tell at a glance that the problem with nnmrules server 290, and thus with group container ManageX-Servers 250, is caused by

nnmrules:CPU health characteristic 312. Next, in order to determine the exact cause of the poor CPU utilization health status of nnmrules server 290, the administrator selects nnmrules:CPU health characteristic 312. As shown in Figure 12, this causes a pop-up window 320 to appear within GUI 300. Window 320 displays a detailed message made up of information 322-332 to the administrator about the cause of the problem, reflective of the last trap generated by poor CPU utilization. In this example, a critical event occurred on February 7, 2000 at 12:41 PM (information 322). The source of the problem was the NNMRULES server (information 324) and the critical event had to do with message transmittal (information 326). The critical event identification number is 2341 (information 328); the event ID number can be used to further track the critical event if

desired. The computer server affected was the NNMRULES server 312 (information 330). The following is the description or message of the problem (information 332): "CPU responding too low, message server prbs" Once the administrator has read the message displayed within window 320, the OK button 334 can be selected to exit window 320. At any time, the contents of the registration file of a group view may be viewed by selecting Map from the toolbar 340. In Figure 13, the configuration enrollment blocks or contents 360 of the registration file for the MS Exchange-Servers group view and the contents 370 of the registration file for the ManageX group view are shown in window 350. As stated previously, the network objects displayed within a group view are sorted according to their attributes. Additionally, information about the name, background graphic, symboltypes, context, and health indicators (characteristics) may be learned by viewing the contents of a group view's registration file. The above description, taken in conjunction with the drawings, defines an invention that offers various advantages in the art. There is a direct correlation between alarm indicators and the occurrence of an event or trap that caused the alarm to be generated. Previously, while an indicator, such as color of an icon, could be used to indicate poor network object health in general, there was no way to easily and readily directly correlate that indicator to the cause of the problem. Drilling-down on icons indicated as having health concerns allows the administrator or perhaps other user of the network to not only trace the problem to a specific network object and its attendant health characteristics, but to receive detailed information, in the form of a message, that is specific to the actual critical event or condition responsible for the poor health of the object. The solution provided by the present invention is highly proactive, able to automatically detect and communicate present or potential problem areas to a network administrator for immediate correction, potentially before end users are impacted.

[0062] While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.

[SUBMITTED AS ATTACHMENT 2 TO THE FIRST PRELIMINARY AMENDMENT FILED IN
CONTINUATION APPLICATION TO U.S. PATENT APPLICATION 09/523,387.]

[illegible]

**A METHOD AND APPARATUS [STRUCTURE] FOR DYNAMICALLY
DRILLING-DOWN THROUGH A HEALTH MONITORING MAP TO
DETERMINE THE HEALTH STATUS AND CAUSE OF HEALTH PROBLEMS
ASSOCIATED WITH NETWORK OBJECTS OF A MANAGED NETWORK
ENVIRONMENT**

5

RELATED APPLICATIONS

[0001] The present invention is a continuation of copending U.S. Patent
Application No. 09/523,387 filed on March 10, 2000, which is a continuation-in-part of
10 U.S. Patent Application 09/087,338 filed on May 29, 1998.

BACKGROUND OF THE INVENTION

[FIELD OF THE INVENTION]

Field of the Invention

15 [0002] The present invention relates generally to network management, and more particularly, to monitoring health problems of network devices and services of a managed network environment.

[BACKGROUND OF THE INVENTION]

20 **Related Art**

[0003] As computer networks have become more prevalent in corporate and other operating environments, network management software that is capable of solving network problems automatically and remotely has become more crucial. One of the major goals of any efficient network administration setup is the specification and measurement of
25 acceptable performance thresholds for each machine in the network without creating additional network traffic. Network management software typically manages and automates administrative tasks across multiple machines in a network. Typical network management software allows administrators to measure log events and view status when performance criteria is not acceptable. Unfortunately, however, the administrator is often

not informed of problems on the network by network management software until after one or more end users of the network has been affected

[0004] Accordingly, there exists a need in the art for a proactive diagnosis of network management problems in a timely manner. There is further a need for a complete, global
5 view of the network environment, including a view of all critical components. There exists a need to quickly display to the administrator of a network health problems associated with devices and services on the network and provide the capability of the administrator to quickly respond to and correct pending network problems before end users of the network are impacted.

10 [0005] The Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP) are network management protocols that provide a generic mechanism by which different manufacturers' equipment and/or services can be monitored and controlled from a management system, such as a UNIX server. A network component or service provided on a managed network can be
15 monitored and controlled using a management protocol to communicate management information between network components and services on the network. A network component can include networked personal computers, workstations, servers, routers, bridges, print servers, print queues, and printers. Network services, particularly in an Internet environment, can include electronic mail (e-mail), browsers, and service level
20 agreements. There exist several key areas of network management including fault management, configuration management, security management, performance management, and accounting management. With the ability to instruct a network component to report events and the ability to start processes on a network component, the network can be manipulated to suit changing conditions within a network system.

25 [0006] A key mechanism by which various network devices communicate with a management system is via SNMP traps or CMIP events. Hereafter, "events" will be used to refer to either SNMP traps or CMIP events. Events allow for unsolicited notifications to be sent from one network device or service to another. This same mechanism can be used for communication between various cooperating software components within the
30 management system.

[0007] There are several software products that receive events and allow a user to manage network devices. One of these products, Network Node Manager (NNM) from Hewlett-Packard Company of Palo Alto, CA., enables a user to manage network devices using a graphical user interface (GUI) along with graphically representing relationships between network devices. Hereafter "NNM" will be used to generically refer to a product that receives events and allows a user to manage network devices, such as HP's Network Node Manager. From the NNM console, a user is able to discover and display all of the network devices on the network and to proactively monitor and manage all servers on the network. This makes it easy to determine the network status or to follow the path of a failed print job, for instance, and determine the point at which it failed. Because it is easy for a user to see how a network is configured, it is easy to manage network devices and optimize the configuration. For instance, a configuration may be optimized by balancing the number of print queues per print server or the number of print servers per file server. Any network device may be managed by an NNM such as NetWare[®] file servers, print servers, print queues, and printers. (NetWare is a trademark of Novell, Inc.) During initialization of the NNM, network devices are automatically discovered and added to a topology database. Each network device is graphically represented by an icon on the NNM console. Using NNM, a user can proactively monitor and manage all network devices on a managed network. A user can monitor the state on a network device over various periods of time by keeping trend data. A user can use trend thresholds to troubleshoot problems on network devices or to plan future expansion of network devices, such as increasing volume and disk sizes, or increasing the number of users allowed access to a server at one time.

[0008] All events are assigned a default severity which can be overridden by the user. The NNM utilizes registration files for user configurable information. The severity level of each event that is received by the NNM that corresponds to a particular network device is represented by a unique color. The severity level of a network device is indicated on the NNM console by the color of the network device's icon. A critical event, for instance, is depicted with a red icon. For instance, by default, a critical event is indicated to the user when a network device icon on the NNM map changes color to red indicating a critical status related to that network device. Thus, the current status of the

entire network can be easily inspected by a user using the color status indications of the network device icons.

[0009] While the occurrence of a critical event for a network device is depicted by a red icon or other indication for that device, the simple color indication of a red icon, for instance, does not, in and of itself, communicate to the user exactly the nature of the critical event that caused the icon to change to a red color. There is an unmet need in the art for a user, such as an administrator of the network environment, to be able to not only know that the icon for a particular device indicates the occurrence of a critical event, but to also be able to quickly and readily ascertain the exact nature of that critical event.

[0010] Network printers are graphically represented with a printer icon representing each of the network printers on the network. A user can remotely determine the "health" status of any of the network printers visually. The LED status on the network printer can then be browsed to determine if the printer needs to be serviced or if human intervention is required. For instance, it can be determined if a printer has any of the following problems: Out of paper; Out of ink; Paper jam; Door open; Toner low; Printer problem; and Bin full. A drawback of this approach, however, is that the exact nature of the critical event, e.g. door open, has to be determined by looking at the problem network printer device itself and cannot be determined remotely by looking at the red color icon of the problem network printer on the NNM network console.

[0011] Servers are graphically represented with a server icon representing each of the servers on the network. A server running the appropriate agent software may be managed by a user from the NNM console. A server running the appropriate agent software responds to management data requests from the NNM console and transmits alarms from the server to the NNM console. This makes it possible for the NNM to display real-time server performance and configuration data on those servers and to monitor key performance statistics including: CPU utilization; number of users; number of connections; memory usage and configuration; installed software; and disk and volume usage. Thresholds can be set on these parameters to cause an SNMP trap, or they can be graphed by the NNM to evaluate history or trends. Parts of a server may also be viewed when troubleshooting a problem. Viewing components of a server's configuration (the network interfaces, for example) might help solve a critical problem with the server.

[0012] Server faults may be managed by monitoring key parameters of the servers, such as CPU load and available disk space, as well as noting significant events, such as NetWare Loadable Modules (NLMs) being unloaded or trustee rights changing. These conditions may be monitored directly at the servers and passed to the NNM via SNMP traps. For file servers, a user can obtain current and historical trend data and set alarm thresholds for trend parameters so that the user is notified when a threshold is passed.

[0013] Novell's NetWare Management Agent (NMA) Management Information Base (MIBs) and trap definitions are integrated into NNM. NNM may be configured to integrate the NMA traps with associated Novel "NetExpert" help text. When an SNMP alarm is sent to an NNM console, the alarm can be reviewed for more detailed help text describing the problem. The alarm, however, is [if] not directly correlated to the red icon indicating that a particular network device is having a problem. This means that the process of reviewing the alarm sent to the NNM console is separate from the process of viewing a red icon on the NNM console and that these processes are not correlated. The user can also followed detailed instructions that guide the user through a series of steps to resolve the problem discovered by the NMA agent.

[0014] Referring to Figure 3, IP-centric group views 60 for graphically displaying network devices, according to the prior art, is shown. User interface 62 contains a representation of the network indicated by IP Internet icon 64. Double-clicking the IP Internet icon 64 will result in the presentation of user interface 66 having containers 68, 70 for the group views of the network indicated by NW-Servers:GOTO icon 68 and NT-Servers:GOTO icon 70. Double-clicking on NW-Servers:GOTO icon 68 will result in the presentation of user interface 72 containing the NW-Server-related [NW-Servers related] network devices discovered by NNM during initialization. Three NW-Server-related [NW-Servers related] network device icons [devices] are shown each representing individual network devices: nwstrn0a icon 74, nwstrn0b icon 76, and nsmdem3 icon 78. This group view configuration is considered IP-centric (Internet Protocol Centric) because during network device discovery all network devices are initially contained in a single group view that is presented by double-clicking on the IP Internet icon 64. A user may manually construct basic group views such as NW-Servers and NT-Servers as shown as NW-Servers:GOTO icon 68 and NT-Servers:GOTO icon 70, respectively.

[0015] NodeView is a product that enhances products that receive events and allow a user to manage network devices such as NNM. Using NodeView, related network devices are automatically grouped into maps represented by group icons. Group views are hardwired into the NodeView code itself. Referring to Figure 4, device-centric group views 80 for graphically displaying network devices, according to the prior art, is shown. User interface 82 contains a representation of the network on top of background 91, a map of the United States. The top-level network is indicated by Internet icon 84. The group views of the network are represented by NW-Servers icon 90, NT-Servers icon 92, Web-Servers icon 86, HP-Printers icon 88, and DMI-Clients icon 94. This group view configuration is considered device-centric because during network device discovery related network devices are automatically grouped into group views represented by group view icons. Double clicking on a group icon will explode a map, hereafter referred to as a "group view", showing all the related devices that were previously discovered in the topology database. For instance, double-clicking on NW-Servers icon 90 will explode to a NetWare Servers group view showing all of the NetWare servers that were discovered in the topology database. A group view of related devices provides a user with a simple way to monitor and launch applications using the menubar and NetWare tool launcher from a single view of the managed environment. The menubars, popup menus, and toolbar remain consistent for each of the group views provided by NodeView.

[0016] In the prior art, the group views are hardwired into the NodeView code itself. This means that a NodeView user cannot select his/her own choices for group views nor dynamically update this selection. There is therefore an unmet need in the art to allow a user to be able to dynamically configure group view information. Additionally, the menubars, popup menus, and toolbar are not individually configured for a selected group view, but rather remain consistent regardless of whether an item is only applicable for certain group views and meaningless for others. There is therefore an unmet need in the art to allow the menubars, popup menus, and toolbar to be context sensitive to the group view.

SUMMARY OF THE INVENTION

[0017] It is therefore an object of the present invention to quickly display to the administrator of a managed network health problems associated with devices and services on the network and to provide the administrator with the capability to quickly respond to and correct pending network problems before end users of the network are impacted.

[0018] It is a further object of the present invention to allow for a proactive diagnosis of network management problems in a timely manner.

[0019] It is another object of the present to provide a complete, global view of the network environment, including the ability to provide a view of all critical components readily upon demand, to allow for this proactive diagnosis.

[0020] It is yet another object of the present invention to be able to readily and quickly ascertain the exact nature of a critical event that caused an icon representative of a network device or service to change to indicate the occurrence of the critical event.

[0021] Therefore, according to the present invention, user-configurable group views allow an administrator of the network, upon noticing that an icon is indicative of a critical event having occurred, as reflected in the color, shape, or other such indicator of the icon, to "drill down" via a user interface to the network device or service that is the subject of the critical event and to then view an event or trap message associated with the critical event that is stored as a field of the network device or service effected by the critical event. According to the methodology of the present invention, health characteristics of each network object of interest in the network environment that determine the health status of each network object are defined. Each network object is grouped in a group view with other network objects that share attribute values that define the group view. The health characteristics of each network object are monitored in order to determine the health status of each health characteristic of each network object. Moreover, the health characteristics are stored in a health characteristic configuration file, such as a registration file, of a group view with which the network object it is associated with belongs. Group view containers of a map, each corresponding to a group view having a number of network objects within it all sharing common group attribute values,

are displayed within the user interface. The health characteristics, the network objects, and the group view containers each have health status indicators that reflect health status. Health status indicators are intended to quickly convey to the user of the managed network, such as the administrator of the network, when a group view container, network object, or health characteristic is in poor health and may include the color or shape of an icon or an audible alarm. Determining the health status of each health characteristic includes comparing performance data of the health characteristic to a predetermined threshold of the health characteristic, and then, if the performance data of the health characteristic violates the predetermined threshold of the health characteristic, causing the health status indicator of the health characteristic to indicate a poor health condition of the health characteristic. Each group view displayed within the map that has a poor health status is identified by the health status indicator of its container. Selecting the container having a poor health indication, will cause the group view of that container to be displayed within the user interface. The user can quickly tell which of the network objects of the group view have poor health from the health status indicators of the network objects. Selecting the one or more objects having poor health will cause the health characteristics of the problem network objects to be displayed in the user interface. The one or more health characteristics having health problems, as indicated by the health status indicators of the health characteristics, can then be selected to cause a message to be displayed in the user interface that identified the event that caused the poor health status of each health characteristic of concern.

[0022] The drill-down of the present invention to determine the underlying, root cause of a poor health status need not start at the group view container level of the network hierarchy. If the user of the system is already viewing the network objects of a particular group view or the health characteristics of a particular network object, for instance, the drill-down would commence at that level.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The novel features believed characteristic of the invention are set forth in the claims. The invention itself, however, as well as the preferred mode of use, and further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawing(s), wherein:

[0024] Figure 1a illustrates a flow chart of dynamically adding group views, according to the present invention;

[0025] Figure 1b illustrates a flow chart of dynamically modifying group views, according to the present invention;

[0026] Figure 1c illustrates a flow chart of dynamically deleting group views, according to the present invention;

[0027] Figure 2 illustrates a flow chart of the context sensitive menubars, popup menus, and toolbar, according to the present invention;

[0028] Figure 3 illustrates IP-centric group views for graphically displaying network devices, according to the prior art; Figure 4 illustrates device-centric group views for graphically displaying related network devices, according to the prior art;

[0029] Figure 5 illustrates a menubar that is context sensitive to the group view that is selected, according to the present invention;

[0030] Figure 6 illustrates editing group view information that is stored in a file using a graphically interface, according to the present invention

[0031] Figure 7 illustrates of flow chart of dynamically drilling-down through a hierarchy of maps and sub-maps of a managed network to determine health status and causes of health problems associated with network objects of the managed network, according to the present invention;

[0032] Figure 8 illustrates a flow chart of determining health status of health characteristics of network objects, according to the present invention;

[0033] Figure 9 illustrates a group view container and group view Internet map [210] within a graphical user interface, in accordance with an embodiment of the present invention;

[0034] Figure 10 illustrates a group view sub-map containing health status
5 information, in accordance with the present invention;

[0035] Figure 11 illustrates the health characteristics of a network object, in accordance with the present invention; Figure 12 illustrates a user interface that contains a message communicating the cause of a health problem of a network object, in accordance with the present invention; and

10 [0036] Figure 13 illustrates contents of a registration file of user-configurable group views, in accordance with the present invention.

DESCRIPTION OF THE INVENTION

15 [0037] The present invention stores group view information, called group view attributes, in a file that may be edited by a NNM user so that a user can dynamically configure group view information. Group view attributes that may be edited include: the name of the group view, the background graphic image, the symbol type, and the context of the group view. NodeView utilizes registration files to create context sensitive group
20 views such that only those items of a menubar, popup menu, or toolbar that are registered to a particular group view are shown when that group view is selected by the user. These user-configurable group views allow an administrator of the network, upon noticing that an icon is indicative of a critical event having occurred, as reflected in the color, shape, or other such indicator of the icon, to "drill down" to the network device or service that is
25 the subject of the critical event and to then view an event or trap message associated with the critical event that is stored as a field of the network device or service effected by the critical event.

[0038] Referring to Figure 1a, a flow chart of dynamically adding group views 10, according to one embodiment of the present invention, is shown. Initially, the user is
30 presented with a list of group views at Block 12. The user selects to add a group view at

Block 14. The user enters new group view information at Block 16. At Block 18 the new group view is added to the list of group views. Finally, at Block 20, the user is presented with a list of group views including the new group view.

[0039] Referring to Figure 1b, a flow chart of dynamically modifying group views
5 30, according to the present invention, is shown. Initially, the user is presented with a list of group views at Block 32. The user selects to modify a group view at Block 34. The user modifies the group view information at Block 36. The user is again presented with a list of group views at Block 38.

[0040] Referring to Figure 1c, a flow chart of dynamically deleting group views
10 40, according to the present invention, is shown. Initially, the user is presented with a list of group views at Block 42. The user selects to delete a group view at Block 44. The user is presented with a list of the remaining group views at Block 46.

[0041] Referring to Figure 2, a flow chart of the context sensitive menubars,
popup menus, and toolbar 50, according to the present invention, is shown. The user
15 opens a group view, at Block 52, by double-clicking on the group view icon. A lookup is performed on a NodeView registration file for the context sensitive information for that group view at Block 54. The menubars, popup menus, and toolbar for that group view are modified at Block 56.

[0042] Referring to Figure 5, a menubar that is context sensitive to the group view
20 that is selected [60,] according to the present invention, is shown. Double-clicking on NW-Servers icon 90 will result in the presentation of user interface 102 containing the NW-Servers-related network devices discovered by the NodeView-enhanced NNM during initialization. Selecting menubar 104 will result in the presentation of a menubar that is context sensitive to the group view selected, in this case NW-Servers.

[0043] Referring to Figure 6, an illustration of editing group view information,
25 stored in a file, using a graphical user interface 110, according to the present invention, is shown. Selecting map properties from the menubar will result in the presentation of user interface 112 containing Configurable Applications selection list 114. Selecting NodeView from the Configurable Applications selection list 114 will result in the
30 presentation of user interface 116 containing the group view attribute list 118. Group

attributes are listed by name 120 and value 122. A group view attribute may be edited by selecting a group view attribute from the group view attribute list 118 and modifying that group view attribute's value.

[0044] The user-configurable group views described above allow an administrator of the network, upon noticing that an icon of a user interface of the NNM console is indicative of a critical event having occurred, as reflected in the color, shape, or other such indicator of the icon, to "drill down" to the network device or service (object) that is the subject of the critical event and to then view an event or trap message associated with the critical event that is stored as a field of the network device or service effected by the critical event.

[0045] Referring now to Figure 7, the general methodology 130 of a preferred embodiment of the present invention for proactively determining health status of network objects and user-configurable group views of a windows-based managed network environment is shown. It is noted at the outset of the description of Figure 7, that not all steps shown therein are necessarily performed in order to determine the root cause of concern; the amount of drill-down that is required is a function of where in the hierarchy of maps and sub-maps the administrator is located when initially alerted to the presence of a network object in poor health. Similarly, additional steps that those detailed in Figure 7 may be required if the hierarchy of maps and sub-maps of the managed network so dictates; this is accomplished without departing from the spirit and scope of the invention. At Block 140, one or more health characteristics are defined for each network object of interest in the managed network environment.

[0046] As previously stated, network objects of the managed network environment may include network devices such as personal computers, workstations, servers, routers, printers, bridges, etc. and network services such as the Internet and electronic mail. Health characteristics, referred to as "Health Indicators" in the figures, [Figure X,] provide information about the health of a particular network object and can include CPU utilization, memory utilization, network utilization, and disk utilization. For instance, if the network object is a network server, for instance, health characteristics may include disk utilization, memory utilization, network utilization, and processor utilization. The health status of each health characteristic of the network object of interest must be

determined at Block 150. Each health characteristic has a health status that is reflected in a health status indicator; the health status of each health characteristic of a network object is used to determine the health status of the network object, and the health status of each network object of a grouped view (sub-map) is in turn used to determine the overall health status of that group view

[0047] In the preferred embodiment of the present invention, determining the health status of each health characteristic is accomplished in the manner set forth in the methodology 150 of Figure 8 by monitoring the health indicators previously defined. At Block 152, performance data related to the health characteristic of the network object of interest is compared to a preset (predetermined) threshold value of that health characteristic to determine if there is a problem. As an example, when a service level availability threshold in an electronic mail, Internet environment is violated (such that there is less than 90% availability for e-mail), health status indicators notify the administrator of the existence of a problem so that its root cause may be determined timely by drilling down through any sub-maps that exist in the hierarchy of the network.

[0048] If the performance data indicates that performance of the network object, as indicated by the performance data violating the preset threshold value for that health characteristic at Block 154, then the health status indicator of that health characteristic is changed to reflect a poor health status at Block 158. If, however, the performance data does not violate the threshold value then the health status indicator of the health characteristic is reflective of a good health status at Block 156. The health status indicator of a health characteristic may be a color of an icon of the health characteristic, a shape of the icon of the health characteristic, a sound associated with the health characteristic, or other appropriate indicators of health. For instance, the health status indicator may be the color red for the health characteristic icon of interest, the health characteristic icon shaped like a stop sign, or an audible alarm.

[0049] Moreover, indicators capable of communicating varying degrees of trouble may be utilized. Thus, a red icon may be used to indicate a more serious health problem than an orange or yellow icon, for example. Referring back to Figure 7, at Block 160, the health indicators for each network object of interest are stored in a registration file of the appropriate group view; each group view has a registration file database used to store the

attributes and health characteristics, or indicators, associated with all network objects within that group view. It is noted that the order of Blocks 150 and 160 of Figure 7 may be reversed without departing from the spirit and scope of the invention.

[0050] Once the health characteristics of the network objects of interest have been defined and their health status determined, then the “drill down” process of proactively determining problem network objects of the managed network environment may commence. The first step is for a user of the system, such as the system administrator, to have notification that there is a problem of some sort with the network so that the process of proactively determining what the problem [is] can begin. The initial indication of a network problem typically occurs at a high level and the system administrator would then “drill down” to find the specific cause of the problem using the user-configurable group views described earlier.

[0051] At Block 170, group view containers are displayed within a map of the user interface. Each group view container corresponds to a group view, or sub-map, in which network objects sharing the user-definable group view attributes described above and stored in a database are grouped. Each group view container displayed in the user interface has a group view health status indicator that is representative of the overall health status of its group view; the overall health status of the group view is determined by the health status of each network object of the network objects within the group view and the health status of each network object is determined by the health status of the health characteristics of a network object. As with the health status indicator of a health characteristic, the group view health status indicator may be color, shape, sound, or other indicator chosen to be appropriate to the particular network.

[0052] The user can select, through manipulation of the network user interface, one or more group view containers indicated to have an overall health problem at Block 180. Selection of the group view containers occurs within the preferred embodiment by clicking on the container of interest with a mouse within a window of a graphical user interface (GUI); one skilled in the art, however, will recognize that selection may occur through other means as well. Selection of a group view container causes the group view corresponding to that container to be displayed in the user interface. This is the first part of the drill-down process.

[0053] Because the group view container selected has an overall health problem as reflected in its group view health status indicator, at least one network object of the network objects displayed in the group view will also have poor health as reflected in the network object health status indicator of the network object. As with the health status indicator of a health characteristic and the group view health status indicator of a group view, a network object health status indicator may be color, shape, sound, or other indicator chosen to be appropriate to the particular network. At Block 190, the administrator or other user of the network will select the one or more network objects of the group view having a health problem; this is the next step of the drill-down process. Selecting a problem network object will cause one or more health characteristics of the object to be displayed within the user interface; because the network object thus selected has a health problem, at least one of the health characteristics of the network object will in turn have a health status indicator indicative of poor health. The health of each health characteristic thus displayed may be quickly and easily ascertained by its health status indicator, whether that be color, shape, sound, etc.

[0054] Now that one or more health characteristics of a network object have been found to have poor health on the network, the next and final step is to ascertain the root cause of health problem. This is accomplished, at Block 200, by selecting the health characteristic of concern in order to determine its health problem. Selection of a problem health characteristic will cause a message, indicative of the root health problem, to be displayed within the user interface. Typically, the message will be a trap or event message reflective of the critical event that caused the health problem and is stored as a field of the network object.

[0055] The message may be generated for any event type, including SNMP traps and CMIP events. If the invention is being used as part of an alarm browser, such as in Internet applications, the trap message may be stored in the alarm browser.

[0056] It is noted that the administrator of the managed network is provided initial indication of a network problem via the health status indicators of either the group view containers, the network objects within the group view containers, or the health characteristics of the network objects. If the administrator is away from the NNM console, however, the occurrence of the performance data of a health characteristic of a

network object violating a preset threshold value may operate to cause the administrator to be alerted at a remote location, such as by paging the administrator upon the occurrence of the critical event. This allows the critical event to be addressed as soon as possible in order to minimize negative impact on the end users of the network.

5 [0057] It is further noted that depending upon where the administrator is located within the hierarchy of maps (group view containers), sub-maps (group view of network objects), and health characteristics when performance of a network object fails to meet the preset standard for it, a complete drill-down may not be necessary to determine the root cause of the failure. Thus, for instance, an administrator who is looking at a group view
10 sub-map of print servers when a particular print server in that group view has an icon that changes from a green to a red state (change of its network object health status indicator) will be automatically alerted at that level of the hierarchy that a problem exists and thus a complete drill-down from the group view containers is not necessary. The administrator would simply select the problem print server to see which of its health characteristics is
15 indicated as being in poor health. The problem with the health characteristic would be displayed in a trap message after selecting the problem health characteristic as described above. In this example, at least one step of drill-down is eliminated.

[0058] Similarly, if the administrator is already viewing the health characteristics of a particular network object when the health status indicator of one of the health
20 characteristics indicates trouble, the user would only have to select the problem health characteristic to then immediately view a message in the user interface about the critical event. By the same token, the drill-down described in Figures 7 and 8 does not prevent the user of a larger hierarchy of maps and sub-maps to be employed. In fact, there may be additional hierarchical layers of maps and sub-maps beyond that reflected in flow 130
25 without departing from the spirit and scope of the invention.

[0059] An example of a specific implementation that might be used with the present invention is shown in Figures 9-13. In this example, the health status indicators for group view containers, group view network objects, and health characteristics are color-based. Referring now to Figure 9, a group view container and group view Internet
30 map 210 within a graphical user interface 220 is shown. Map 210 illustrates a number of network objects, including Internet network devices 230, 232, 234, 236, 238, 240, 242,

244, and 246, as well as group view containers 248 and 250. All of the network objects in map 210 have a green health status indicator, except for 232 which is yellow; group view container 248 for ManageX-Servers has a brown indicator while group view container for MS Exchange-Servers 250 has a red indicator. Also illustrated are the alarm categories 215 utilized in an alarm browser on the Internet. Error Alarms, Status Alarms, and Application Alert are indicated by the color brown in the alarm browser. Threshold alarms and All alarms are indicated by the color red in the alarm browser. ManageX and MS Exchange alarms are indicated by green in the alarm browser.

[0060] Of particular concern in map 210 is ManageX-Servers group view container 250, which is red in color, an indication that there is a potentially serious health problem with one or more of the network objects contained within container 250. Selecting container 250, such as by clicking on it, brings up the group view or sub-map 260 of the ManageX-Servers within the GUI 265 of Figure 10; this is the first drill-down step in this example. Within group view 260 there are shown three ManageX-Servers: hpdaver server 270, nnmrules server 290, and theforce server 280. At a glance, a network administrator can see which of the servers contained within group view 260 has a health problem. hpdaver and theforce servers 270, 280 are both green, while nnmrules server 290 is blue. The blue network object health status indicator of nnmrules server 290 is the color blue, an indication of a poor health condition in this example.

[0061] The administrator thus selects nnmrules server 290, such as by clicking on it with a point-and-click device, to drill-down to the health characteristics of this network device in Figure 11. Displayed within GUI 300 are various health characteristics 310: nnmrules:CPU health characteristic 312, nnmrules:Disk health characteristic 314, nnmrules:Memory health characteristic 316, and nnmrules:Network health characteristic 318; as previously discussed, these health characteristics refer to CPU utilization, disk utilization, memory utilization, and network utilization, respectively. Only nnmrules:CPU health characteristic 312 has a health status indicator that is red; the health status indicators of the other health characteristics are green. Since red denotes an alarm in this example, the administrator can tell at a glance that the problem with nnmrules server 290, and thus with group container ManageX-Servers 250, is caused by nnmrules:CPU health characteristic 312. Next, in order to determine the exact cause of

the poor CPU utilization health status of nmmrules server 290, the administrator selects nmmrules:CPU health characteristic 312. As shown in Figure 12, this causes a pop-up window 320 to appear within GUI 300. Window 320 displays a detailed message made up of information 322-332 to the administrator about the cause of the problem, reflective of the last trap generated by poor CPU utilization. In this example, a critical event occurred on February 7, 2000 at 12:41 PM (information 322). The source of the problem was the NNMRULES server (information 324) and the critical event had to do with message transmittal (information 326). The critical event identification number is 2341 (information 328); the event ID number can be used to further track the critical event if desired. The computer server affected was the NNMRULES server 312 (information 330). The following is the description or message of the problem (information 332): "CPU responding too low, message server prbs" Once the administrator has read the message displayed within window 320, the OK button 334 can be selected to exit window 320. At any time, the contents of the registration file of a group view may be viewed by selecting Map from the toolbar 340. In Figure 13, the configuration enrollment blocks or contents 360 of the registration file for the MS Exchange-Servers group view and the contents 370 of the registration file for the ManageX group view are shown in window 350. As stated previously, the network objects displayed within a group view are sorted according to their attributes. Additionally, information about the name, background graphic, symboltypes, context, and health indicators (characteristics) may be learned by viewing the contents of a group view's registration file. The above description, taken in conjunction with the drawings, defines an invention that offers various advantages in the art. There is a direct correlation between alarm indicators and the occurrence of an event or trap that caused the alarm to be generated. Previously, while an indicator, such as color of an icon, could be used to indicate poor network object health in general, there was no way to easily and readily directly correlate that indicator to the cause of the problem. Drilling-down on icons indicated as having health concerns allows the administrator or perhaps other user of the network to not only trace the problem to a specific network object and its attendant health characteristics, but to receive detailed information, in the form of a message, that is specific to the actual critical event or condition responsible for the poor health of the object. The solution provided by the present invention is highly proactive, able to automatically detect and communicate

present or potential problem areas to a network administrator for immediate correction, potentially before end users are impacted.

[0062] While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that
5 various changes in form and detail may be made therein without departing from the spirit and scope of the invention.

10990318-2

1 **A METHOD AND STRUCTURE FOR DYNAMICALLY DRILLING-**
2 **DOWN THROUGH A HEALTH MONITORING MAP TO DETERMINE**
3 **THE HEALTH STATUS AND CAUSE OF HEALTH PROBLEMS**
4 **ASSOCIATED WITH NETWORK OBJECTS OF A MANAGED**
5 **NETWORK ENVIRONMENT**

6
7 **Cross-Reference to Related Application**

8 This application is a continuation-in-part of co-pending United States Patent
9 Application Serial No. 09/087,338, filed on May 29, 1998.
10

11 **FIELD OF THE INVENTION**

12
13 The present invention relates generally to network management, and more
14 particularly to monitoring health problems of network devices and services of a
15 managed network environment.

16
17 **BACKGROUND OF THE INVENTION**

18
19 As computer networks have become more prevalent in corporate and other
20 operating environments, network management software that is capable of solving
21 network problems automatically and remotely has become more crucial. One of
22 the major goals of any efficient network administration setup is the specification
23 and measurement of acceptable performance thresholds for each machine in the
24 network without creating additional network traffic. Network management software
25 typically manages and automates administrative tasks across multiple machines in
26 a network. Typical network management software allows administrators to
27 measure log events and view status when performance criteria is not acceptable.
28 Unfortunately, however, the administrator is often not informed of problems on the
29 network by network management software until after one or more end users of the
30 network has been affected.

31
32 Accordingly, there exists a need in the art for a proactive diagnosis of
33 network management problems in a timely manner. There is further a need for a
34 complete, global view of the network environment, including a view of all critical

1 components. There exists a need to quickly display to the administrator of a
2 network health problems associated with devices and services on the network and
3 provide the capability of the administrator to quickly respond to and correct pending
4 network problems before end users of the network are impacted.

5
6 The Simple Network Management Protocol (SNMP) and Common
7 Management Information Protocol (CMIP) are network management protocols that
8 provide a generic mechanism by which different manufacturers' equipment and/or
9 services can be monitored and controlled from a management system, such as a
10 UNIX server. A network component or service provided on a managed network
11 can be monitored and controlled using a management protocol to communicate
12 management information between network components and services on the
13 network. A network component can include networked personal computers,
14 workstations, servers, routers, bridges, print servers, print queues, and printers.
15 Network services, particularly in an Internet environment, can include electronic
16 mail (e-mail), browsers, and service level agreements. There exist several key
17 areas of network management including fault management, configuration
18 management, security management, performance management, and accounting
19 management. With the ability to instruct a network component to report events and
20 the ability to start processes on a network component, the network can be
21 manipulated to suit changing conditions within a network system.

22
23 A key mechanism by which various network devices communicate with a
24 management system is via SNMP traps or CMIP events. Hereafter, "events" will be
25 used to refer to either SNMP traps or CMIP events. Events allow for unsolicited
26 notifications to be sent from one network device or service to another. This same
27 mechanism can be used for communication between various cooperating software
28 components within the management system.

29
30 There are several software products that receive events and allow a user to
31 manage network devices. One of these products, Network Node Manager (NNM)
32 from Hewlett-Packard Company of Palo Alto, CA., enables a user to manage

1 network devices using a graphical user interface (GUI) along with graphically
2 representing relationships between network devices. Hereafter "NNM" will be used
3 to generically refer to a product that receives events and allows a user to manage
4 network devices, such as Network Node Manager. From the NNM console, a user
5 is able to discover and display all of the network devices on the network and to
6 proactively monitor and manage all servers on the network. This makes it easy to
7 determine the network status or to follow the path of a failed print job, for instance,
8 and determine the point at which it failed. Because it is easy for a user to see how
9 a network is configured, it is easy to manage network devices and optimize the
10 configuration. For instance, a configuration may be optimized by balancing the
11 number of print queues per print server or the number of print servers per file
12 server. Any network device may be managed by NNM such as NetWare file
13 servers, print servers, print queues, and printers. During initialization of NNM,
14 network devices are automatically discovered and added to a topology database.
15 Each network device is graphically represented by an icon on the NNM console.

16
17 Using NNM, a user can proactively monitor and manage all network devices
18 on a managed network. A user can monitor the state on a network device over
19 various periods of time by keeping trend data. A user can use trend thresholds to
20 troubleshoot problems on network devices or to plan future expansion of network
21 devices, such as increasing volume and disk sizes, or increasing the number of
22 users allowed access to a server at one time.

23
24 All events are assigned a default severity which can be overridden by the
25 user. NNM utilizes registration files for user configurable information. The severity
26 level of each event that is received by NNM that corresponds to a particular
27 network device is represented by a unique color. The severity level of a network
28 device is indicated on the NNM console by the color of the network device's icon.
29 A critical event, for instance, is depicted with a red icon. For instance, by default, a
30 critical event is indicated to the user when a network device icon on the NNM map
31 changes color to red indicating a critical status related to that network device.

1 Thus, the current status of the entire network can be easily inspected by a user
2 using the color status indications of the network device icons.

3
4 While the occurrence of a critical event for a network device is depicted by a
5 red icon or other indication for that device, the simple color indication of a red icon,
6 for instance, does not, in and of itself, communicate to the user exactly the nature
7 of the critical event that caused the icon to change to a red color. There is an
8 unmet need in the art for a user, such as an administrator of the network
9 environment, to be able to not only know that the icon for a particular device
10 indicates the occurrence of a critical event, but to also be able to quickly and
11 readily ascertain the exact nature of that critical event.

12
13 Network printers are graphically represented with a printer icon representing
14 each of the network printers on the network. A user can remotely determine the
15 "health" status of any of the network printers visually. The LED status on the
16 network printer can then be browsed to determine if the printer needs to be
17 serviced or if human intervention is required. For instance, it can be determined if a
18 printer has any of the following problems: Out of paper; Out of ink; Paper jam; Door
19 open; Toner low; Printer problem; and Bin full. A drawback of this approach,
20 however, is that the exact nature of the critical event, e.g. door open, has to be
21 determined by looking at the problem network printer device itself and cannot be
22 determined remotely by looking at the red color icon of the problem network printer
23 on the NNM network console.

24
25 Servers are graphically represented with a server icon representing each of
26 the servers on the network. A server running the appropriate agent software may
27 be managed by a user from the NNM console. A server running the appropriate
28 agent software responds to management data requests from the NNM console and
29 transmits alarms from the server to the NNM console. This makes it possible for
30 NNM to display real-time server performance and configuration data on those
31 servers and to monitor key performance statistics including: CPU utilization;
32 number of users; number of connections; memory usage and configuration;

1 installed software; and disk and volume usage. Thresholds can be set on these
2 parameters to cause an SNMP trap, or they can be graphed by NNM to evaluate
3 history or trends. Parts of a server may also be viewed when troubleshooting a
4 problem. Viewing components of a server's configuration (the network interfaces,
5 for example) might help solve a critical problem with the server.
6

7 Server faults may be managed by monitoring key parameters of the servers,
8 such as CPU load and available disk space, as well as noting significant events,
9 such as NetWare Loadable Modules (NLMs) being unloaded or trustee rights
10 changing. These conditions may be monitored directly at the servers and passed
11 to the NNM via SNMP traps. For file servers, a user can obtain current and
12 historical trend data and set alarm thresholds for trend parameters so that the user
13 is notified when a threshold is passed.
14

15 Novell's NetWare Management Agent (NMA) Management Information Base
16 (MIBs) and trap definitions are integrated into NNM. NNM may be configured to
17 integrate the NMA traps with associated Novel "NetExpert" help text. When an
18 SNMP alarm is sent to an NNM console, the alarm can be reviewed for more
19 detailed help text describing the problem. The alarm, however, if not directly
20 correlated to the red icon indicating that a particular network device is having a
21 problem. This means that the process of reviewing the alarm sent to the NNM
22 console is separate from the process of viewing a red icon on the NNM console
23 and that these processes are not correlated. The user can also followed detailed
24 instructions that guide the user through a series of steps to resolve the problem
25 discovered by the NMA agent.
26

27 Referring to **Figure 3**, IP-centric group views 60 for graphically displaying
28 network devices, according to the prior art, is shown. User interface 62 contains a
29 representation of the network indicated by IP Internet icon 64. Double-clicking the
30 IP Internet icon 64 will result in the presentation of user interface 66 having
31 containers 68, 70 for the group views of the network indicated by
32 NW-Servers:GOTO icon 68 and NT-Servers:GOTO icon 70. Double-clicking on

1 NW-Servers:GOTO icon 68 will result in the presentation of user interface 72
2 containing the NW-Servers related network devices discovered by NNM during
3 initialization. Three NW-Servers related network devices are shown each
4 representing individual network devices: nwstrn0a icon 74, nwstrn0b icon 76, and
5 nsmdem3 icon 78. This group view configuration is considered IP-centric (Internet
6 Protocol Centric) because during network device discovery all network devices are
7 initially contained in a single group view that is presented by double-clicking on the
8 IP Internet icon 64. A user may manually construct basic group views such as NW-
9 Servers and NT-Servers as shown as NW-Servers:GOTO icon 68 and
10 NT-Servers:GOTO icon 70, respectively.

11
12 NodeView is a product that enhances products that receive events and allow
13 a user to manage network devices such as NNM. Using NodeView, related
14 network devices are automatically grouped into maps represented by group icons.
15 Group views are hardwired into the NodeView code itself. Referring to **Figure 4**,
16 device-centric group views 80 for graphically displaying network devices, according
17 to the prior art, is shown. User interface 82 contains a representation of the
18 network on top of background 91, a map of the United States. The top-level
19 network is indicated by Internet icon 84. The group views of the network are
20 represented by NW-Servers icon 90, NT-Servers icon 92, Web-Servers icon 86,
21 HP-Printers icon 88, and DMI-Clients icon 94. This group view configuration is
22 considered device-centric because during network device discovery related
23 network devices are automatically grouped into group views represented by group
24 view icons. Double clicking on a group icon will explode a map, hereafter referred
25 to as a "group view", showing all the related devices that were previously
26 discovered in the topology database. For instance, double-clicking on NW-Servers
27 icon 90 will explode to a NetWare Servers group view showing all of the NetWare
28 servers that were discovered in the topology database. A group view of related
29 devices provides a user with a simple way to monitor and launch applications using
30 the menubar and NetWare tool launcher from a single view of the managed
31 environment. The menubars, popup menus, and toolbar remain consistent for
32 each of the group views provided by NodeView.

1
2 In the prior art, the group views are hardwired into the NodeView code itself.
3 This means that a NodeView user cannot select his/her own choices for group
4 views nor dynamically update this selection. There is therefore an unmet need in
5 the art to allow a user to be able to dynamically configure group view information.
6 Additionally, the menubars, popup menus, and toolbar are not individually
7 configured for a selected group view, but rather remain consistent regardless of
8 whether an item is only applicable for certain group views and meaningless for
9 others. There is therefore an unmet need in the art to allow the menubars, popup
10 menus, and toolbar to be context sensitive to the group view.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to quickly display to the administrator of a managed network health problems associated with devices and services on the network and to provide the administrator with the capability to quickly respond to and correct pending network problems before end users of the network are impacted.

It is a further object of the present invention to allow for a proactive diagnosis of network management problems in a timely manner.

It is another object of the present to provide a complete, global view of the network environment, including the ability to provide a view of all critical components readily upon demand, to allow for this proactive diagnosis.

It is yet another object of the present invention to be able to readily and quickly ascertain the exact nature of a critical event that caused an icon representative of a network device or service to change to indicate the occurrence of the critical event.

Therefore, according to the present invention, user-configurable group views allow an administrator of the network, upon noticing that an icon is indicative of a critical event having occurred, as reflected in the color, shape, or other such indicator of the icon, to "drill down" via a user interface to the network device or service that is the subject of the critical event and to then view an event or trap message associated with the critical event that is stored as a field of the network device or service effected by the critical event. According to the methodology of the present invention, health characteristics of each network object of interest in the network environment that determine the health status of each network object are defined. Each network object is grouped in a group view with other network objects that share attribute values that define the group view. The health characteristics of each network object are monitored in order to determine the

1 health status of each health characteristic of each network object. Moreover, the
2 health characteristics are stored in a health characteristic configuration file, such as
3 a registration file, of a group view with which the network object it is associated with
4 belongs. Group view containers of a map, each corresponding to a group view
5 having a number of network objects within it all sharing common group attribute
6 values, are displayed within the user interface. The health characteristics, the
7 network objects, and the group view containers each have health status indicators
8 that reflect health status. Health status indicators are intended to quickly convey to
9 the user of the managed network, such as the administrator of the network, when a
10 group view container, network object, or health characteristic is in poor health and
11 may include the color or shape of an icon or an audible alarm. Determining the
12 health status of each health characteristic includes comparing performance data of
13 the health characteristic to a predetermined threshold of the health characteristic,
14 and then, if the performance data of the health characteristic violates the
15 predetermined threshold of the health characteristic, causing the health status
16 indicator of the health characteristic to indicate a poor health condition of the health
17 characteristic.

18
19 Each group view displayed within the map that has a poor health status is
20 identified by the health status indicator of its container. Selecting the container
21 having a poor health indication, will cause the group view of that container to be
22 displayed within the user interface. The user can quickly tell which of the network
23 objects of the group view have poor health from the health status indicators of the
24 network objects. Selecting the one or more objects having poor health will cause
25 the health characteristics of the problem network objects to be displayed in the
26 user interface. The one or more health characteristics having health problems, as
27 indicated by the health status indicators of the health characteristics, can then be
28 selected to cause a message to be displayed in the user interface that identified
29 the event that caused the poor health status of each health characteristic of
30 concern.
31

1 The drill-down of the present invention to determine the underlying, root
2 cause of a poor health status need not start at the group view container level of the
3 network hierarchy. If the user of the system is already viewing the network objects
4 of a particular group view or the health characteristics of a particular network
5 object, for instance, the drill-down would commence at that level.

10990318-1

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the claims. The invention itself, however, as well as the preferred mode of use, and further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawing(s), wherein:

Figure 1a illustrates a flow chart of dynamically adding group views, according to the present invention;

Figure 1b illustrates a flow chart of dynamically modifying group views, according to the present invention;

Figure 1c illustrates a flow chart of dynamically deleting group views, according to the present invention;

Figure 2 illustrates a flow chart of the context sensitive menubars, popup menus, and toolbar, according to the present invention;

Figure 3 illustrates IP-centric group views for graphically displaying network devices, according to the prior art;

Figure 4 illustrates device-centric group views for graphically displaying related network devices, according to the prior art;

Figure 5 illustrates a menubar that is context sensitive to the group view that is selected, according to the present invention;

Figure 6 illustrates editing group view information that is stored in a file using a graphically interface, according to the present invention;

1 **Figure 7** illustrates of flow chart of dynamically drilling-down through a
2 hierarchy of maps and sub-maps of a managed network to determine health status
3 and causes of health problems associated with network objects of the managed
4 network, according to the present invention;

5
6 **Figure 8** illustrates a flow chart of determining health status of health
7 characteristics of network objects, according to the present invention;

8
9 **Figure 9** illustrates a group view container and group view Internet map 210
10 within a graphical user interface, in accordance with an embodiment of the present
11 invention;

12
13 **Figure 10** illustrates a group view sub-map containing health status
14 information, in accordance with the present invention;

15
16 **Figure 11** illustrates the health characteristics of a network object, in
17 accordance with the present invention;

18
19 **Figure 12** illustrates a user interface that contains a message
20 communicating the cause of a health problem of a network object, in accordance
21 with the present invention; and

22
23 **Figure 13** illustrates contents of a registration file of user-configurable group
24 views, in accordance with the present invention.

DESCRIPTION OF THE INVENTION

The present invention stores group view information, called group view attributes, in a file that may be edited by a NNM user so that a user can dynamically configure group view information. Group view attributes that may be edited include: the name of the group view, the background graphic image, the symbol type, and the context of the group view. NodeView utilizes registration files to create context sensitive group views such that only those items of a menubar, popup menu, or toolbar that are registered to a particular group view are shown when that group view is selected by the user. These user-configurable group views allow an administrator of the network, upon noticing that an icon is indicative of a critical event having occurred, as reflected in the color, shape, or other such indicator of the icon, to "drill down" to the network device or service that is the subject of the critical event and to then view an event or trap message associated with the critical event that is stored as a field of the network device or service effected by the critical event.

Referring to **Figure 1a**, a flow chart of dynamically adding group views 10, according to the present invention, is shown. Initially, the user is presented with a list of group views at Block 12. The user selects to add a group view at Block 14. The user enters new group view information at Block 16. At Block 18 the new group view is added to the list of group views. Finally, at Block 20, the user is presented with a list of group views including the new group view.

Referring to **Figure 1b**, a flow chart of dynamically modifying group views 30, according to the present invention, is shown. Initially, the user is presented with a list of group views at Block 32. The user selects to modify a group view at Block 34. The user modifies the group view information at Block 36. The user is again presented with a list of group views at Block 38.

Referring to **Figure 1c**, a flow chart of dynamically deleting group views 40, according to the present invention, is shown. Initially, the user is presented with a

1 list of group views at Block 42. The user selects to delete a group view at Block
2 44. The user is presented with a list of the remaining group views at Block 46.

3
4 Referring to **Figure 2**, a flow chart of the context sensitive menubars, popup
5 menus, and toolbar 50, according to the present invention, is shown. The user
6 opens a group view, at Block 52, by double-clicking on the group view icon. A
7 lookup is performed on a NodeView registration file for the context sensitive
8 information for that group view at Block 54. The menubars, popup menus, and
9 toolbar for that group view are modified at Block 56.

10
11 Referring to **Figure 5**, a menubar that is context sensitive to the group view
12 that is selected 60, according to the present invention, is shown. Double-clicking
13 on NW-Servers icon 90 will result in the presentation of user interface 102
14 containing the NW-Servers related network devices discovered by the NodeView
15 enhanced NNM during initialization. Selecting menubar 104 will result in the
16 presentation of a menubar that is context sensitive to the group view selected, in
17 this case NW-Servers.

18
19 Referring to **Figure 6**, an illustration of editing group view information, stored
20 in a file, using a graphical user interface 110, according to the present invention, is
21 shown. Selecting map properties from the menubar will result in the presentation
22 of user interface 112 containing Configurable Applications selection list 114.
23 Selecting NodeView from the Configurable Applications selection list 114 will result
24 in the presentation of user interface 116 containing the group view attribute list
25 118. Group attributes are listed by name 120 and value 122. A group view
26 attribute may be edited by selecting a group view attribute from the group view
27 attribute list 118 and modifying that group view attribute's value.

28
29 The user-configurable group views described above allow an administrator
30 of the network, upon noticing that an icon of a user interface of the NNM console is
31 indicative of a critical event having occurred, as reflected in the color, shape, or
32 other such indicator of the icon, to "drill down" to the network device or service

1 (object) that is the subject of the critical event and to then view an event or trap
2 message associated with the critical event that is stored as a field of the network
3 device or service effected by the critical event.
4

5 Referring now to **Figure 7**, the general methodology 130 of a preferred
6 embodiment of the present invention for proactively determining health status of
7 network objects and user-configurable group views of a windows-based managed
8 network environment is shown. It is noted at the outset of the description of Figure
9 7, that not all steps shown therein are necessarily performed in order to determine
10 the root cause of concern; the amount of drill-down that is required is a function of
11 where in the hierarchy of maps and sub-maps the administrator is located when
12 initially alerted to the presence of a network object in poor health. Similarly,
13 additional steps that those detailed in Figure 7 may be required if the hierarchy of
14 maps and sub-maps of the managed network so dictates; this is accomplished
15 without departing from the spirit and scope of the invention. At Block 140, one or
16 more health characteristics are defined for each network object of interest in the
17 managed network environment. As previously stated, network objects of the
18 managed network environment may include network devices such as personal
19 computers, workstations, servers, routers, printers, bridges, etc. and network
20 services such as the Internet and electronic mail. Health characteristics, referred
21 to as "Health Indicators" in Figure X, provide information about the health of a
22 particular network object and can include CPU utilization, memory utilization,
23 network utilization, and disk utilization. For instance, if the network object is a
24 network server, for instance, health characteristics may include disk utilization,
25 memory utilization, network utilization, and processor utilization. The health status
26 of each health characteristic of the network object of interest must be determined at
27 Block 150. Each health characteristic has a health status that is reflected in a
28 health status indicator; the health status of each health characteristic of a network
29 object is used to determine the health status of the network object, and the health
30 status of each network object of a grouped view (sub-map) is in turn used to
31 determine the overall health status of that group view.
32

1 In the preferred embodiment of the present invention, determining the health
2 status of each health characteristic is accomplished in the manner set forth in the
3 methodology 150 of **Figure 8** by monitoring the health indicators previously
4 defined. At Block 152, performance data related to the health characteristic of the
5 network object of interest is compared to a preset (predetermined) threshold value
6 of that health characteristic to determine if there is a problem. As an example,
7 when a service level availability threshold in an electronic mail, Internet
8 environment is violated (such that there is less than 90% availability for e-mail),
9 health status indicators notify the administrator of the existence of a problem so
10 that its root cause may be determined timely by drilling down through any sub-
11 maps that exist in the hierarchy of the network. If the performance data indicates
12 that performance of the network object, as indicated by the performance data
13 violating the preset threshold value for that health characteristic at Block 154, then
14 the health status indicator of that health characteristic is changed to reflect a poor
15 health status at Block 158. If, however, the performance data does not violate the
16 threshold value then the health status indicator of the health characteristic is
17 reflective of a good health status at Block 156. The health status indicator of a
18 health characteristic may be a color of an icon of the health characteristic, a shape
19 of the icon of the health characteristic, a sound associated with the health
20 characteristic, or other appropriate indicators of health. For instance, the health
21 status indicator may be the color red for the health characteristic icon of interest,
22 the health characteristic icon shaped like a stop sign, or an audible alarm.
23 Moreover, indicators capable of communicating varying degrees of trouble may be
24 utilized. Thus, a red icon may be used to indicate a more serious health problem
25 than an orange or yellow icon, for example. Referring back to Figure 7, at Block
26 160, the health indicators for each network object of interest are stored in a
27 registration file of the appropriate group view; each group view has a registration
28 file database used to store the attributes and health characteristics, or indicators,
29 associated with all network objects within that group view. It is noted that the order
30 of Blocks 150 and 160 of Figure 7 may be reversed without departing from the
31 spirit and scope of the invention.
32

1 Once the health characteristics of the network objects of interest have been
2 defined and their health status determined, then the "drill down" process of
3 proactively determining problem network objects of the managed network
4 environment may commence. The first step is for a user of the system, such as the
5 system administrator, to have notification that there is a problem of some sort with
6 the network so that the process of proactively determining what the problem is can
7 begin. The initial indication of a network problem typically occurs at a high level
8 and the system administrator would then "drill down" to find the specific cause of
9 the problem using the user-configurable group views described earlier. At Block
10 170, group view containers are displayed within a map of the user interface. Each
11 group view container corresponds to a group view, or sub-map, in which network
12 objects sharing the user-definable group view attributes described above and
13 stored in a database are grouped. Each group view container displayed in the user
14 interface has a group view health status indicator that is representative of the
15 overall health status of its group view; the overall health status of the group view is
16 determined by the health status of each network object of the network objects
17 within the group view and the health status of each network object is determined by
18 the health status of the health characteristics of a network object. As with the
19 health status indicator of a health characteristic, the group view health status
20 indicator may be color, shape, sound, or other indicator chosen to be appropriate to
21 the particular network.

22
23 The user can select, through manipulation of the network user interface, one
24 or more group view containers indicated to have an overall health problem at Block
25 180. Selection of the group view containers occurs within the preferred
26 embodiment by clicking on the container of interest with a mouse within a window
27 of a graphical user interface (GUI); one skilled in the art, however, will recognize
28 that selection may occur through other means as well. Selection of a group view
29 container causes the group view corresponding to that container to be displayed in
30 the user interface. This is the first part of the drill-down process. Because the
31 group view container selected has an overall health problem as reflected in its
32 group view health status indicator, at least one network object of the network

1 objects displayed in the group view will also have poor health as reflected in the
2 network object health status indicator of the network object. As with the health
3 status indicator of a health characteristic and the group view health status indicator
4 of a group view, a network object health status indicator may be color, shape,
5 sound, or other indicator chosen to be appropriate to the particular network. At
6 Block 190, the administrator or other user of the network will select the one or more
7 network objects of the group view having a health problem; this is the next step of
8 the drill-down process. Selecting a problem network object will cause one or more
9 health characteristics of the object to be displayed within the user interface;
10 because the network object thus selected has a health problem, at least one of the
11 health characteristics of the network object will in turn have a health status
12 indicator indicative of poor health. The health of each health characteristic thus
13 displayed may be quickly and easily ascertained by its health status indicator,
14 whether that be color, shape, sound, etc.

15
16 Now that one or more health characteristics of a network object have been
17 found to have poor health on the network, the next and final step is to ascertain the
18 root cause of health problem. This is accomplished, at Block 200, by selecting the
19 health characteristic of concern in order to determine its health problem. Selection
20 of a problem health characteristic will cause a message, indicative of the root
21 health problem, to be displayed within the user interface. Typically, the message
22 will be a trap or event message reflective of the critical event that caused the health
23 problem and is stored as a field of the network object. The message may be
24 generated for any event type, including SNMP traps and CMIP events. If the
25 invention is being used as part of an alarm browser, such as in Internet
26 applications, the trap message may be stored in the alarm browser.

27
28 It is noted that the administrator of the managed network is provided initial
29 indication of a network problem via the health status indicators of either the group
30 view containers, the network objects within the group view containers, or the health
31 characteristics of the network objects. If the administrator is away from the NNM
32 console, however, the occurrence of the performance data of a health

1 characteristic of a network object violating a preset threshold value may operate to
2 cause the administrator to be alerted at a remote location, such as by paging the
3 administrator upon the occurrence of the critical event. This allows the critical
4 event to be addressed as soon as possible in order to minimize negative impact on
5 the end users of the network.
6

7 It is further noted that depending upon where the administrator is located
8 within the hierarchy of maps (group view containers), sub-maps (group view of
9 network objects), and health characteristics when performance of a network object
10 fails to meet the preset standard for it, a complete drill-down may not be necessary
11 to determine the root cause of the failure. Thus, for instance, an administrator who
12 is looking at a group view sub-map of print servers when a particular print server in
13 that group view has an icon that changes from a green to a red state (change of its
14 network object health status indicator) will be automatically alerted at that level of
15 the hierarchy that a problem exists and thus a complete drill-down from the group
16 view containers is not necessary. The administrator would simply select the
17 problem print server to see which of its health characteristics is indicated as being
18 in poor health. The problem with the health characteristic would be displayed in a
19 trap message after selecting the problem health characteristic as described above.
20 In this example, at least one step of drill-down is eliminated. Similarly, if the
21 administrator is already viewing the health characteristics of a particular network
22 object when the health status indicator of one of the health characteristics indicates
23 trouble, the user would only have to select the problem health characteristic to then
24 immediately view a message in the user interface about the critical event. By the
25 same token, the drill-down described in Figures 7 and 8 does not prevent the user
26 of a larger hierarchy of maps and sub-maps to be employed. In fact, there may be
27 additional hierarchical layers of maps and sub-maps beyond that reflected in flow
28 130 without departing from the spirit and scope of the invention.
29

30 An example of a specific implementation that might be used with the present
31 invention is shown in Figures 9-13. In this example, the health status indicators for
32 group view containers, group view network objects, and health characteristics are

1 color-based. Referring now to **Figure 9**, a group view container and group view
2 Internet map 210 within a graphical user interface 220 is shown. Map 210
3 illustrates a number of network objects, including Internet network devices 230,
4 232, 234, 236, 238, 240, 242, 244, and 246, as well as group view containers 248
5 and 250. All of the network objects in map 210 have a green health status
6 indicator, except for 232 which is yellow; group view container 248 for ManageX-
7 Servers has a brown indicator while group view container for MS Exchange-
8 Servers 250 has a red indicator. Also illustrated are the alarm categories 215
9 utilized in an alarm browser on the Internet. Error Alarms, Status Alarms, and
10 Application Alert are indicated by the color brown in the alarm browser. Threshold
11 alarms and All alarms are indicated by the color red in the alarm browser.
12 ManageX and MS Exchange alarms are indicated by green in the alarm browser.

13
14 Of particular concern in map 210 is ManageX-Servers group view container
15 250, which is red in color, an indication that there is a potentially serious health
16 problem with one or more of the network objects contained within container 250.
17 Selecting container 250, such as by clicking on it, brings up the group view or sub-
18 map 260 of the ManageX-Servers within the GUI 265 of **Figure 10**; this is the first
19 drill-down step in this example. Within group view 260 there are shown three
20 ManageX-Servers: hpdaver server 270, nnmrules server 290, and theforce server
21 280. At a glance, a network administrator can see which of the servers contained
22 within group view 260 has a health problem. hpdaver and theforce servers 270,
23 280 are both green, while nnmrules server 290 is blue. The blue network object
24 health status indicator of nnmrules server 290 is the color blue, an indication of a
25 poor health condition in this example.

26
27 The administrator thus selects nnmrules server 290, such as by clicking on it
28 with a point-and-click device, to drill-down to the health characteristics of this
29 network device in **Figure 11**. Displayed within GUI 300 are various health
30 characteristics 310: nnmrules:CPU health characteristic 312, nnmrules:Disk health
31 characteristic 314, nnmrules:Memory health characteristic 316, and
32 nnmrules:Network health characteristic 318; as previously discussed, these health

1 characteristics refer to CPU utilization, disk utilization, memory utilization, and
2 network utilization, respectively. Only nnmrules:CPU health characteristic 312 has
3 a health status indicator that is red; the health status indicators of the other health
4 characteristics are green. Since red denotes an alarm in this example, the
5 administrator can tell at a glance that the problem with nnmrules server 290, and
6 thus with group container ManageX-Servers 250, is caused by nnmrules:CPU
7 health characteristic 312. Next, in order to determine the exact cause of the poor
8 CPU utilization health status of nnmrules server 290, the administrator selects
9 nnmrules:CPU health characteristic 312. As shown in **Figure 12**, this causes a
10 pop-up window 320 to appear within GUI 300. Window 320 displays a detailed
11 message made up of information 322-332 to the administrator about the cause of
12 the problem, reflective of the last trap generated by poor CPU utilization. In this
13 example, a critical event occurred on February 7, 2000 at 12:41 PM (information
14 322). The source of the problem was the NNMRULES server (information 324)
15 and the critical event had to do with message transmittal (information 326). The
16 critical event identification number is 2341 (information 328); the event ID number
17 can be used to further track the critical event if desired. The computer server
18 affected was the NNMRULES server 312 (information 330). The following is the
19 description or message of the problem (information 332): "CPU responding too low,
20 message server prbs" Once the administrator has read the message displayed
21 within window 320, the OK button 334 can be selected to exit window 320.

22
23 At any time, the contents of the registration file of a group view may be
24 viewed by selecting Map from the toolbar 340. In **Figure 13**, the configuration
25 enrollment blocks or contents 360 of the registration file for the MS Exchange-
26 Servers group view and the contents 370 of the registration file for the ManageX
27 group view are shown in window 350. As stated previously, the network objects
28 displayed within a group view are sorted according to their attributes. Additionally,
29 information about the name, background graphic, symboltypes, context, and health
30 indicators (characteristics) may be learned by viewing the contents of a group
31 view's registration file.

1 The above description, taken in conjunction with the drawings, defines an
2 invention that offers various advantages in the art. There is a direct correlation
3 between alarm indicators and the occurrence of an event or trap that caused the
4 alarm to be generated. Previously, while an indicator, such as color of an icon,
5 could be used to indicate poor network object health in general, there was no way
6 to easily and readily directly correlate that indicator to the cause of the problem.
7 Drilling-down on icons indicated as having health concerns allows the administrator
8 or perhaps other user of the network to not only trace the problem to a specific
9 network object and its attendant health characteristics, but to receive detailed
10 information, in the form of a message, that is specific to the actual critical event or
11 condition responsible for the poor health of the object. The solution provided by
12 the present invention is highly proactive, able to automatically detect and
13 communicate present or potential problem areas to a network administrator for
14 immediate correction, potentially before end users are impacted.

15
16 While the invention has been particularly shown and described with
17 reference to a preferred embodiment, it will be understood by those skilled in the
18 art that various changes in form and detail may be made therein without departing
19 from the spirit and scope of the invention.
20